International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

# An Energy Efficient WSN through Watchdog Optimization

**Muhammed Swalih .K .T[1], Akila .M[2]**

[1]PG Scholar, Rathinam Technical Campus, Coimbatore-21, India

[2]Assistant Professor, Dept. of ECE, Rathinam Technical Campus, Coimbatore-21, India

**Abstract:** ***The technique of using watchdog is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). But this kind of technique consumes much energy and hence largely limits the lifespan of WSN. Although the researches in this field realized the importance of trust system's efficiency in WSNs and proposed several solutions which are not sufficient for achieving maximum efficiency. So they have overlooked to optimize the watchdog technique, which is perhaps among the top energy consuming units. The inefficient use of watchdog technique is used in existing trust systems. Thereby this proposed method is a suite of optimization methods to minimize the energy consumption of watchdog usage, while keeping the security of whole system in a sufficient level. Here the concept contributions of this project consist of theoretical analyses and practical algorithms, which can effectively and efficiently schedule the watchdog tasks depending on the sensor node's locations and the target node's trustworthiness. Implementing and simulating the project is done using Network simulator, to assess its real time working and performance evaluation.***

**Keyword*:*** WSN, Watchdog, Optimization Suite, Trust system

## 1. Introduction

The main aim of this project is to ensure the energy efficiency in a wireless sensor network. The inefficient use of watchdog implementation in existing trust systems lead me to propose a suite of optimization methods to minimize the energy consumption of watchdog, while keeping a sufficient level system security. The optimization method consist of theoretical analyses and practical algorithms, which can effectively and efficiently schedule the watchdog tasks depending on the sensor node's locations and the target node's trustworthiness.

More precisely, sensor nodes are usually equipped with limited energy and they have to work as unattended for a long period in various isolated terrains. To adapt various harsh environments is a critical factor which determines the efficiency of whole system. Replacement or recharging of those node's power is very expensive and difficult. The proposed method's energy saving can play an important role in the design of modern WSNs.Anyhow no existing system give appropriate solutions to save the energy consumed by the watchdog technique. The optimization of watchdog can significantly improve the efficiency in a significant manner throughout the Wireless Sensor Network and energy consumption can also optimized. This is done in NS2 in Ubuntu OS and the output is simulated to analyse the performance.

## 2. Proposed System

The goal of this project is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping robustness and trust accuracy in a sufficient level. To touch this goal, we can optimize the technique of implementing watchdog in two levels.

At First the watchdog locations are optimized by considering the fact that, the sensor nodes which are located closely may consume less energy and to monitor each other due to shorter communication distance between them. So these nodes are more likely of being compromised themselves and cause collaborative attacks. Therefore explore the optimal watchdog location to minimize the overall risk (in terms of both security and energy consumption).

Second, the watchdog frequency is optimized and reduce its redundancy. The watchdog frequency and redundancy optimization can reduce the energy consumption and increase the efficiency of the whole system of WSN.

## 3. Analysis of the System Design and its Implementation

Input design is the primary part of overall design of the system, which requires very careful attention. If the data going into the system are incorrect and then processing the output will magnify these errors.

The inputs in the system are of three types:
•External: Prime inputs to the system
•Internal: User communication
• Interactive: Inputs entered during a dialog.

The above input types enrich the proposed system with numerous facilities that make it more advantageous in comparison with the existing system design.

All the inputs entered are completely raw, initially, before entering into a database, then each of them available processing.

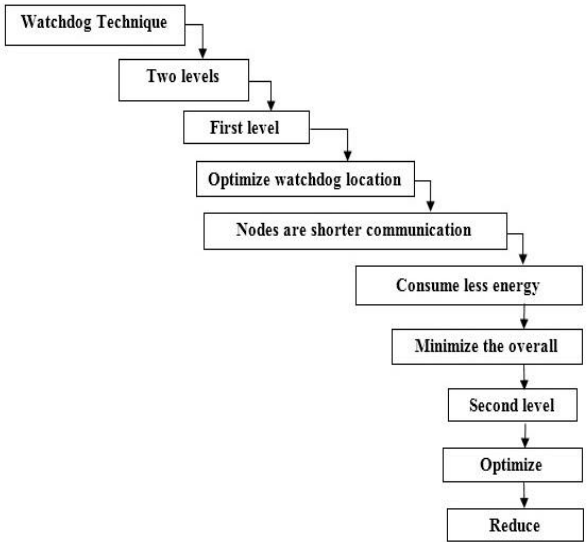



**Figure 1:** Block Diagram of Implementation

The implementation is done as:

- Sensor Nodes deployment and creation of Watchdog nodes
- Watchdog identify the battery level of each sensor and recharge or replace
- Monitor the location of neighbour sensor and communicate
- Short distance communication based clusters to increase efficiency.
- Detecting collaborative attacks for the implemented watchdog technique
- Performance Analysis

### 3.1 Watchdog location optimization

To optimize the location of watchdog, Have to find the optimal Wj , ∀v j ∈ V by directly solving the optimization problem described because they are ill-posed and do not have solution in closed form. To conquer this challenge, we find optimal watchdog positions instead (find optimal dij given ∀v j ∈ V). The selection of neighbour nodes vi ∈ Bj which are located near to the optimal dij is more likely able to form the optimal Wj.

To transform the original optimization problem of finding optimal Wj to the problem of finding optimal dij, the intuitive evidence is that: although the vi ∈ Bj with a less dij will consume less energy to perform watchdog tasks to monitor vj and hence ensure the energy minimization goal in such vi is more likely of being controlled by attackers if v j is an attacker's node.

The use of attacker's node as watchdogs will impede the security maximization goal in since those sensor nodes can report fake watchdog results to drop the trust robustness. We therefore find the optimal watchdog location dij given a target node v j by considering an overall risk, which considers both energy and security.

The Practical Algorithm (DBP Algorithm): Although Theorem gives the optimal watchdog location in theory, it is still challenging to apply this theory as a solution to practical WSN. The reason is that, for almost sensor nodes, we cannot assume there necessarily exist some neighbour nodes located at the optimal watchdog location. In common, almost v j ∈ V may have their neighbours. To address this issue, an intuitive solution is to choose the node nearest to the theoretically optimal location as watchdog. Anyhow, this intuitive algorithm is vulnerable to discrimination attacks. That is, since the intuitive algorithm fixes the watchdog node to v j 's nearest neighbour, v j ∈ A can simply behave well to v j 's nearest node but launch WSN attacks dropping routing packets or reporting dishonest sensing data to the rest of v j 's neighbourhood.

### 3.2 Network Architectures

Sensor nodes, the nodes are either compromised or selfish or on fault. Those nodes can bypass traditional security criteria using their identification, but can be possibly captured by trust systems due to their poor reputation or past misbehaviour. That is, trust is built upon sensor nodes reputation and past behaviours, and can be used to label these node's internal states and honesty. Although many trust systems enable trust recommendations to extend the trust from neighbourhood (i.e., direct trust) to a global network view (i.e., indirect trust), the direct experience of past behaviours is still the basis for securing those recommendations. In another word, sensor node's past behaviours constitute the basic foundation. Collecting enough past behaviours through business traffic to build a reliable trust system for a wireless sensor network is not a trivial task.

First, the network base station when WSN has a flat topology and cluster heads when a hierarchical topology, both of which are likely to have business requirements to interact with the whole network or cluster, may not identify in the communication range of all sensor nodes (i.e., some nodes are remote), so the missing of opportunity to have direct experiences with those remote nodes.

Second, some sensor nodes may not have the requirements to communicate with their neighbour nodes, or their business interactions occur at a very low frequency. Those lazy node's past behaviours are hard to be collected using business traffic.

Third, since trust is context aware, the experience of one kind of behaviours cannot be used to build up trust for another kind. For example, a node behaving well in routing of packets in the past does not mean the sensing data reported from this node is trustworthy (i.e., past multi-hop routing behaviours cannot derive the trust for data sensing).As a result, these wireless sensor network may not contain a vast variety of communication or business traffic to build up all kinds of trust.

To tackle those challenges and facilitate past behaviour collection, most of existing WSNTSs have adopted a so-called watchdog technique. Using this technique, sensor nodes can act and operate as proactive monitors and apply the trust-dedicated tasks in a previously defined frequency to directly communicate or interact with their neighbourhood nodes. Thus they can get the first-hand experiences of these node's behaviours, even if no business tasks happen.

### 3.3 Watchdog optimization

Two ultimate goals when optimizing watchdog techniques: First is to minimize the energy usage or consumption of the whole WSN and the other is to maximize the security (in terms of trust accuracy and trust robustness). The optimization goals as follows: Minimize the energy consumption throughout the whole WSN and maximize trust accuracy of WSN.Hence the Watchdog Optimization is the core area of energy optimization.

### 3.4 Critical design factors

The design of a wireless sensor networks (WSNs) requires a keen knowledge of a variety of vast areas in research fields including wireless communication, networking, digital signal processing and software engineering. However, several factors exist that significantly influence the design of WSNs.The design is done as per the required specification of the required environment.

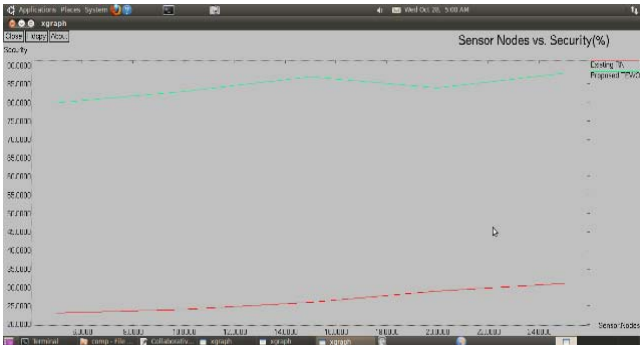
The hardware constraints may lead sensor nodes to frequently fail or might get blocked for a certain interval of time. These faults may occur because of a power faults, physical damage, natural or environment interference or even software problems. The large number of unattended and inaccessible sensor nodes, which are significantly prone to frequent failures, make topology maintenance a challenging task.By optimizing and controlling the energy conception can increase the network life time and the WSN will stay alive than usual can improve its performance.

The successful operation of a Wireless sensor network relies on reliable communication between the nodes in the network. In a multi-hop sensor network, nodes can communicate through a wireless medium creating links between each other. The Watchdog is very significant for an effective Wireless Sensor Network (WSN) to operate under the required level of efficiency and sufficient level of security.

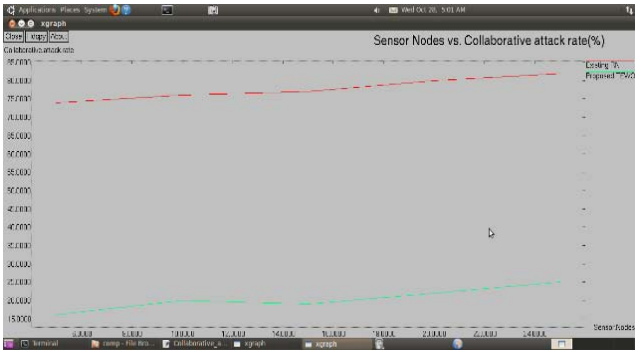
## 4. Performance Analysis

The Performance analysis is done by analysing the output of the existing system with the proposed system performance. It can be analysed effectively using graphical representation of existing and proposed system performance. By analysing the graph in common terms such as the number of nodes is taken here as a large one in order to understand the levels in a real time manner. Here the performance analysis is plotted in NS2 is as follows:

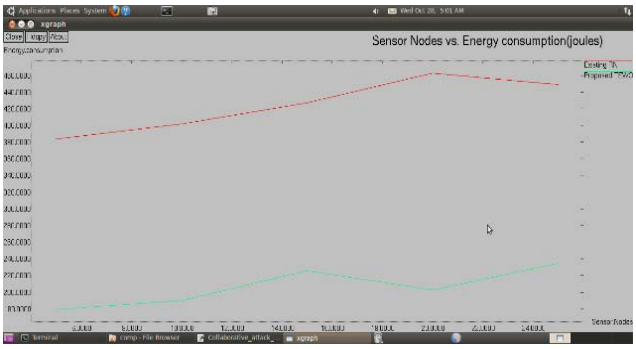
### 4.1 Existing versus Proposed System performance analysis of generated graph.




**Graph 1:** Sensor nodes and Security




**Graph 2:** Sensor nodes and Collaborative attack




**Graph 3:** Sensor nodes and Energy consumption

## 5. Future Enhancements

In future whenever the network demands more efficient system of wireless sensor networks, then the watchdog efficiency can further improved by reducing the energy consumption increasing the speed of action or increased security implementation within the clustered topology of sensor nodes. The higher levels of algorithms are to be developed for achieving those objectives. However the watchdog can remain as the trust system element within the networking of sensors. The Wireless sensor networks will remain as our future communication links in various higher modes of operations even in our space exploration or in secret military operations etc.

## 6. Conclusion

In this work the importance of trust systems efficiency in Wireless sensor networks and several preliminary solutions are overlooked to optimize the energy consumption of watchdog technique, which is perhaps among the top energy-consuming units.

The inefficient and inappropriate use of watchdog technique in existing trust systems leads to propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the security level of whole system in a sufficient level.

## References

[1] Seung-Jun Kim, Xiaodong Wang, and Mohammad Madihian, "Distributed Joint Routing and Medium Access Control for Lifetime Maximization of Wireless Sensor Networks",IEEE transactions on wireless communications, vol. 6, no. 7, July 2007 2669
[2] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Member, IEEE Computer Society,Heejo Lee, Member, IEEE, Sungyoung Lee, Member, IEEE, and Young-Jae Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks" IEEE transactions on parallel and distributed systems, vol. 20, no. 11, Nov 2009
[3] Xiaoyong Li, Feng Zhou, and Junping Du,"LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks",IEEE transactions on information forensics and security, vol. 8, no. 6, June 2013
[4] Yi Ren, Member, IEEE, Vladimir I. Zadorozhny, Senior Member, IEEE,Vladimir A. Oleshchuk, Senior Member, IEEE, and Frank Y. Li, Senior Member, IEEE, "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks" IEEE transactions on mobile computing, vol. 13, no. 7, July 2014
[5] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng. IEEE "Design and Implementation of TARF: A Trust-Aware Routing Framework for wsns", transactions on dependable and secure computing, vol. 9, no. 2, March/April 2012.
[6] Jin-Hee Cho, Member, IEEE, Ananthram Swami, Fellow, IEEE, and Ing-Ray Chen, Member, IEEE. "A Survey on Trust Management for Mobile Ad Hoc Networks", ieee communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011
[7] Manik Lal Das, Member, IEEE, "Two-Factor User Authentication in Wireless Sensor Networks", ieee transactions on wireless commu, vol. 8, no. 3, March 2009
[8] Xiaojiang Du, North Dakota State University Hsiao-Hwa Chen, National Cheng Kung University "Security In Wireless Sensor Networks", IEEE wireless communications August 2008.

## Author Profile

**Mr Muhammed Swalih.K.T** received his B.E degree in Electronics and Communication Engineering (2013) from CMS College of Engineering and Technology, Coimbatore, Affiliated to Anna University, Chennai, Tamilnadu. Currently he is pursuing M.E degree in Applied Electronics from Rathinam Technical Campus, Coimbatore, Affiliated to Anna University Chennai, Tamilnadu. His research interests are High speed Networking and Embedded System.

**MsAkhila.M** received herB.E degree in Electronics and Communication Engineering (2012) and M.E degree in VLSI design (2014) from P.A College of Engineering & Technology, Pollachi, TamilNadu and working as an Assistant Professor in the department of ECE at Rathinam Technical Campus, Coimbatore. Her area of interests are low power VLSI and electronic devices.